The Weight Hierarchy of Some Reducible Cyclic Codes

Maosheng Xiong, Shuxing Li and Gennian Ge

Abstract

The generalized Hamming weights (GHWs) of linear codes are fundamental parameters, the knowledge of which is of great interest in many applications. However, to determine the GHWs of linear codes is difficult in general. In this paper, we study the GHWs for a family of reducible cyclic codes and obtain the complete weight hierarchy in several cases. This is achieved by extending the idea of [57] into higher dimension and by employing some interesting combinatorial arguments. It shall be noted that these cyclic codes may have arbitrary number of nonzeroes.

Index Terms

Cyclic code, exponential sum, generalized Hamming weight, weight hierarchy.

I. INTRODUCTION

Let $\mathcal{C}$ be an $[n, k]$ linear code over the finite field $\mathbb{F}_q$ of order q, that is, $\mathcal{C} \subset \mathbb{F}_q^n$ is a k-dimensional vector space over $\mathbb{F}_q$. For any (linear) subcode $\mathcal{D} \subset \mathcal{C}$, the *support* of $\mathcal{D}$ is defined to be

$$\text{supp}(\mathcal{D}) = \{i : 0 \le i \le n-1, c_i \ne 0 \text{ for some } (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{D}\}.$$

For $1 \le r \le k$, the r-th *generalized Hamming weight* (GHW) of $\mathcal{C}$ is given by

$$d_r(\mathcal{C}) = \min \left\{ |\text{supp}(\mathcal{D})| : \mathcal{D} \subset \mathcal{C} \text{ and } \dim_{\mathbb{F}_q}(\mathcal{D}) = r \right\}.$$

Here $|\text{supp}(\mathcal{D})|$ denotes the cardinality of the set $\text{supp}(\mathcal{D})$. The set $\{d_r(\mathcal{C}) : 1 \le r \le k\}$ is called the *weight hierarchy* of $\mathcal{C}$. Note that $d_1(\mathcal{C})$ is just the minimum distance of $\mathcal{C}$.

Including the minimum distance, the GHWs of linear codes provide additional fundamental information. The notion was introduced by Helleseth, Kløve, and Mykkeltveit [19], [29] and was first used by Wei [53] in cryptography to fully characterize the performance of linear codes when used in a wire-tap channel of type II [37] or as a t-resilient function. The GHWs can be used to characterize the performance of certain secret sharing schemes based on linear codes [30]. Recently, the concept of GHWs has been extended to linear network codes [36], where they were used to characterize the security performance of linear network codes in a wiretap network [39]. Apart from these cryptographic applications, the GHWs also provide detailed structural information of linear codes, the knowledge of the GHWs can be used to

1). compute the state and branch complexity profiles of linear codes [12], [28];
2). indicate efficient ways to shorten linear codes [21];
3). derive subtle upper bounds on the covering radius of linear codes [27];
4). determine the erasure list-decodability of linear codes [15];
5). provide bounds on the list size in the list decoding of certain codes [13], etc.

In conclusion, the GHWs of linear codes provide fundamental parameters of linear codes which are important in many applications.

The study of GHWs has attracted considerable attention in the past two decades, and many results have been obtained in the literature. For example, general lower bounds and upper bounds on GHWs were derived [1], [7], [18], [20], [53], an efficient algorithm to compute the GHWs of cyclic codes was proposed [26], and the GHWs have been determined or estimated for many series of linear codes such as Hamming codes [53], Reed-Muller codes [16], [53], binary Kasami codes [21], Melas and dual Melas codes [45], BCH codes and their duals [4], [6], [10], [11], [33], [42], [46], [48], [49], [52], trace codes [5], [14], [43], [47], [50], product codes [17], [32], [38], [40], [41], [54] and algebraic geometry codes [2], [3], [8], [23], [24], [34], [35], [56], etc. However, generally speaking, computing the GHWs of linear codes is difficult, and the complete weight hierarchy is known for only a few cases (see for example [2], [21], [22], [23], [38], [51], [53], [54], [57]). Interested readers may refer

to Section 7.10 of the excellent textbook [25] for a brief introduction to GHWs, and to [44] for a comprehensive survey of GHWs via a geometric approach.

In a recent interesting paper [57], the authors employed some new ideas from number theory to study the GHWs of irreducible cyclic codes and obtained the weight hierarchy for several cases. Their results extend some previous works [22], [51]. Inspired by this work, in this paper we study the GHWs of a family of reducible cyclic codes which were introduced in [55] where the weight distribution was obtained in several cases. This family of cyclic codes may be characterized as having arbitrary number of nonzeroes and contain as special cases many subfamilies of cyclic codes whose weight distribution was investigated in the literature, and in particular contain the irreducible cyclic codes considered in [57]. We determine the weight hierarchy of this family of cyclic codes in several cases by extending the ideas of [57] into higher dimension and by employing some interesting combinatorial arguments.

We organize the paper as follows. In Section II, we introduce the family of reducible cyclic codes we are interested in and state the main results Theorems 1 and 2. In Section III we briefly introduce some basic concepts and notions which will be used in the proofs. In Section IV we derive an expression of GHWs in terms of Gauss periods. Sections V and VI are devoted to the proofs of parts (i) and (ii) of Theorem 1 respectively. We prove Theorem 2 in Section VII. Section VIII concludes the paper.

II. MAIN RESULTS

Let $q = p^s$, $Q = q^m$ where p is a prime number, s, m are positive integers. Let γ be a primitive element of the finite field $\mathbb{F}_Q$. Assume the following three assumptions:

i) $e \mid (Q - 1)$, $a \not\equiv 0 \pmod{Q - 1}$, $e \geq t \geq 1$;
ii) For $1 \leq i \leq t$, $a_i \equiv a + \frac{Q-1}{e}\Delta_i \pmod{Q-1}$ where $\Delta_i \not\equiv \Delta_j \pmod{e}$ for $i \neq j$ and $\gcd(\Delta_2 - \Delta_1, \ldots, \Delta_t - \Delta_1, e) = 1$;
iii) $\deg h_{a_i}(x) = m$ for $1 \leq i \leq t$ and $h_{a_i}(x) \neq h_{a_j}(x)$ for $i \neq j$. Here $h_a(x)$ denotes the minimal polynomial of γ^{-a} over $\mathbb{F}_q$.

Let us define

$$\delta = \gcd(Q - 1, a_1, a_2, \ldots, a_t),$$

$$n = \frac{Q-1}{\delta}, \qquad N = \gcd\left(\frac{Q-1}{q-1}, ae\right).$$

It is clear that $\delta \mid \frac{Q-1}{e}$ and hence

$$e\delta \mid N(q-1). \tag{1}$$

Under the above three assumptions, we define $\mathcal{C}$ to be the cyclic code of length n over $\mathbb{F}_q$ with parity check polynomial given by $\prod_{i=1}^{t} h_{a_i}(x)$, where a_i's are specified according to the assumptions. It is known that $\mathcal{C}$ is an $[n, tm]$ cyclic code with t nonzeroes.

We remark that this family of cyclic codes were originally defined in [55] in which the weight distribution was obtained in several cases. There is an abundance of $\mathcal{C}$ in the family, given the flexibility of parameters e, t, Δ_i's. In particular, it was observed in [55, Lemma 6] that Assumption iii) always holds true if $N \leq \sqrt{Q}$, which is the case in this paper because we only treat $N = 1, 2$. The main results of the paper are as follows:

Theorem 1. *Let $\mathcal{C}$ be the cyclic code defined as above with $e = t \geq 1$. Let $d_r := d_r(\mathcal{C})$ be the r-th GHW of $\mathcal{C}$.*
(i). If $N = 1$, then we have

$$d_r = \frac{q^m - 1}{\delta}\left(1 - \frac{s}{t}\right) - \frac{q^{(t-s)m-r} - 1}{t\delta}, \quad \text{if } (t-s-1)m < r \leq (t-s)m,$$

where $0 \leq s \leq t - 1$.
(ii). If $N = 2$, then we have

$$d_r = \begin{cases} \frac{q^m - 1}{\delta}(1 - \frac{s}{t}) - \frac{1}{t\delta}(q^{(t-s-\frac{1}{2})m-r} + 1)(q^{\frac{m}{2}} - 1) & \text{if } (t-s-1)m < r \leq \left(t-s-\frac{1}{2}\right)m, \\ \frac{q^m - 1}{\delta}\left(1 - \frac{s}{t}\right) - \frac{2}{t\delta}(q^{(t-s)m-r} - 1) & \text{if } \left(t-s-\frac{1}{2}\right)m < r \leq (t-s)m, \end{cases}$$

where $0 \leq s \leq t - 1$.

Theorem 2. *Let $\mathcal{C}$ be a cyclic code defined as above with $e > t \geq 1$ and $N = 1$. Suppose $\{\Delta_1 \pmod{e}, \ldots, \Delta_t \pmod{e}\}$ is an arithmetic progression. Let $d_r := d_r(\mathcal{C})$ be the r-th GHW of $\mathcal{C}$. Then*

$$d_r = \begin{cases} \frac{q^m - 1}{\delta}(1 - \frac{t-1}{e}) - \frac{e-t+1}{e\delta}(q^{m-r} - 1) & \text{if } 1 \leq r \leq m, \\ \frac{q^m - 1}{\delta}(1 - \frac{s}{e}) - \frac{q^{(t-s)m-r} - 1}{e\delta} & \text{if } (t-s-1)m < r \leq (t-s)m, \end{cases}$$

where $0 \leq s \leq t - 2$.

We remark that when $t = 1$, Theorems 1 and 2 reduce to Corollary 3.2 and Theorem 4.1 of [57] respectively. When $t \geq 2$, the results are new.

It looks likely that the weight hierarchy of $\mathcal{C}$ can still be determined when $e > t \geq 1$ and $N = 2$, however, for a complete answer, the computation becomes quite complicated. We may come back to this problem in the future.

III. PRELIMINARIES

In this section, we introduce some preliminary results which will be used later in the paper.

A. Cyclic Codes

Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Assume that $(n, q) = 1$. $\mathcal{C}$ is called cyclic, if in additional to be linear, $\mathcal{C}$ satisfies the property that the cyclic shift $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. For such a cyclic code $\mathcal{C}$, each codeword $c = (c_0, \ldots, c_{n-1})$ can be associated with a polynomial $\sum_{i=0}^{n-1} c_i x^i$ in the principal ideal ring $R_n := \mathbb{F}_q[x]/(x^n - 1)$. Under this correspondence, $\mathcal{C}$ can be identified with an ideal of R_n. Hence, there is a unique polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(x) \mid x^n - 1$ such that $\mathcal{C} = (g(x))R_n$. The $g(x)$ is called the *generator polynomial* of $\mathcal{C}$, and $h(x) = \frac{x^n - 1}{g(x)}$ is called the *parity check polynomial* of $\mathcal{C}$. When R_n is specified, a cyclic code is uniquely determined by either the generator polynomial or parity check polynomial. $\mathcal{C}$ is said to have i *zeroes* if its generator polynomial can be factorized into a product of i irreducible polynomials over $\mathbb{F}_q$. When the dual code $\mathcal{C}^\perp$ has i zeroes, we call $\mathcal{C}$ a cyclic code with i *nonzeroes*.

B. Group Characters, Gauss Sums and Gauss Periods

Let $q = p^s$ where p is a prime number. The *canonical additive character* ψ_q of $\mathbb{F}_q$ is given by

$$\psi_q : \mathbb{F}_q \longrightarrow \mathbb{C}$$
$$x \mapsto \zeta_p^{\mathrm{Tr}_p^q(x)},$$

where $\zeta_p = \exp\left(2\pi\sqrt{-1}/p\right)$ is a primitive p-th root of unity of $\mathbb{C}$, and Tr_p^q is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. If Q is a power of q, by the transitivity of trace functions we have $\psi_Q = \psi_q \circ \mathrm{Tr}_q^Q$.

Let $\chi : \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \to \mathbb{C}$ be a multiplicative character, that is, $\chi(xy) = \chi(x)\chi(y)$ for any $x, y \in \mathbb{F}_q^*$. We may extend the definition of χ to $\mathbb{F}_q$ by setting $\chi(0) = 0$. The corresponding *Gauss sum* $G(\chi)$ is defined by

$$G(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi_q(x),$$

where ψ is the canonical additive character. If the order of χ equals two, χ is called the quadratic character of $\mathbb{F}_q$ and the corresponding Gauss sum the quadratic Gauss sum. The explicit values of quadratic Gauss sums are known and are recorded as follows.

Lemma 3. [31, Theorem 5.15] *Let $q = p^s$ and χ be the quadratic character of $\mathbb{F}_q$ (hence p is odd). Then*

$$G(\chi) = \begin{cases} (-1)^{s-1}\sqrt{q} & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{s-1}\left(\sqrt{-1}\right)^s \sqrt{q} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Let γ be a primitive element of $\mathbb{F}_q$. For $N \mid (q-1)$, denote by $\langle \gamma^N \rangle$ the multiplicative subgroup generated by γ^N. Then for any $0 \leq i \leq N - 1$, $C_i^{(N,q)} = \gamma^i \langle \gamma^N \rangle$ is called the i-th cyclotomy class of $\mathbb{F}_q$. For any $a \in \mathbb{F}_q$, we define the *Gauss period* $\eta_a^{(N,q)}$ as

$$\eta_a^{(N,q)} = \sum_{x \in C_0^{(N,q)}} \psi_q(ax).$$

IV. AN EXPRESSION OF THE GHWS

Let $\mathcal{C}$ be the cyclic code defined in Introduction. By Delsarte's Theorem [9], elements of $\mathcal{C}$ can be represented uniquely by $c(\underline{x}) = (c_i(\underline{x}))_{i=1}^n$ where $\underline{x} = (x_1, x_2, \ldots, x_t)$ runs over the set $\mathbb{F}_Q^t$ and

$$c_i(\underline{x}) = \mathrm{Tr}_q^Q\left(\sum_{j=1}^t x_j \gamma^{a_j i}\right), \quad 1 \leq i \leq n.$$

In other words, the map

$$\Psi : \mathbb{F}_Q^t \longrightarrow \mathcal{C},$$
$$\underline{x} \mapsto c(\underline{x})$$

is an isomorphism between two $\mathbb{F}_q$-vector spaces $\mathbb{F}_Q^t$ and $\mathcal{C}$, hence induces a 1-1 correspondence between r-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_Q^t$ and r-dimensional subcodes of $\mathcal{C}$ for any $1 \leq r \leq tm$. For any $\mathbb{F}_q$-vector space M, denote by $\begin{bmatrix} M \\ r \end{bmatrix}$ the set of r-dimensional $\mathbb{F}_q$-subspaces of M.

For any $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, define

$$N(H_r) = |\{i : 1 \leq i \leq n, c_i(\underline{b}) = 0, \forall \underline{b} \in H_r\}|,$$

and for any $1 \leq r \leq tm$, define

$$N_r = \max \left\{ N(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}.$$

Since Ψ is an isomorphism, by definition, the r-th GHW of $\mathcal{C}$ can be expressed as

$$d_r := d_r(\mathcal{C}) = n - N_r.$$

Let $\underline{\epsilon_1}, \ldots, \underline{\epsilon_r}$ be an $\mathbb{F}_q$-basis of H_r. Then,

$$c_i(\underline{b}) = 0, \forall \underline{b} \in H_r \iff c_i(\underline{\epsilon_j}) = 0, \forall 1 \leq j \leq r.$$

As before we use ψ_Q (resp. ψ_q) to denote the canonical additive character of $\mathbb{F}_Q$ (resp. $\mathbb{F}_q$). By using orthogonality of ϕ_q we have

$$N(H_r) = \sum_{i=1}^{n} \left\{ \frac{1}{q} \sum_{x_1 \in \mathbb{F}_q} \psi_q(x_1 c_i(\underline{\epsilon_1})) \right\} \cdots \left\{ \frac{1}{q} \sum_{x_r \in \mathbb{F}_q} \psi_q(x_r c_i(\underline{\epsilon_r})) \right\}$$

$$= \frac{1}{q^r} \sum_{i=1}^{n} \sum_{x_1, \ldots, x_r \in \mathbb{F}_q} \psi_q(c_i(x_1 \underline{\epsilon_1} + \cdots + x_r \underline{\epsilon_r}))$$

$$= \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r} \psi_q(c_i(\underline{b})) = \frac{n}{q^r} + \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r^*} \psi_q(c_i(\underline{b})),$$

where $H_r^* = H_r \setminus \{0\}$. Recall that $\gamma^{a_j} = \gamma^{a + \frac{Q-1}{e} \Delta_j}$. By setting $\beta_j = \gamma^{\frac{Q-1}{e} \Delta_j}$, we have $\gamma^{a_j} = \gamma^a \beta_j$. Thus,

$$(q-1)N(H_r) = \frac{n(q-1)}{q^r} + \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r^*} \sum_{x \in \mathbb{F}_q^*} \psi_q(c_i(x\underline{b}))$$

$$= \frac{n(q-1)}{q^r} + \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r^*} \sum_{x \in \mathbb{F}_q^*} \psi_q \left(x \mathrm{Tr}_q^Q \left(\sum_{j=1}^{t} b_j \gamma^{a_j i} \right) \right)$$

$$= \frac{n(q-1)}{q^r} + \frac{1}{q^r} \sum_{\underline{b} \in H_r^*} \sum_{i=1}^{n} \sum_{x \in \mathbb{F}_q^*} \psi_Q \left(x \gamma^{ai} \sum_{j=1}^{t} b_j \beta_j^i \right).$$

Noting that $e \mid \frac{Q-1}{\delta} = n$, any $1 \leq i \leq n$ can be expressed as $i = ej + h$ with $0 \leq j \leq \frac{n}{e} - 1$ and $1 \leq h \leq e$. Thus, the second term on the right can be written as

$$\frac{1}{q^r} \sum_{\underline{b} \in H_r^*} \sum_{j=0}^{\frac{n}{e}-1} \sum_{h=1}^{e} \sum_{x \in \mathbb{F}_q^*} \psi_Q \left(x \gamma^{aej} \gamma^{ah} \sum_{j=1}^{t} b_j \beta_j^h \right).$$

Noting that $\mathbb{F}_q^* = \left\langle \gamma^{\frac{Q-1}{q-1}} \right\rangle$ and $N = \gcd \left(\frac{Q-1}{q-1}, ae \right)$, it is easy to check that

$$\left\{ x \gamma^{aej} \mid x \in \mathbb{F}_q^*, 0 \leq j \leq \frac{n}{e} - 1 \right\} = \frac{(q-1)N}{e\delta} * C_0^{(N,Q)},$$

where we use $l * A$ to denote a multiset whose elements are those of the set A, each repeating l times. Consequently, we have

$$\frac{1}{q^r} \sum_{\underline{b} \in H_r^*} \sum_{j=0}^{\frac{n}{e}-1} \sum_{h=1}^{e} \sum_{x \in \mathbb{F}_q^*} \psi_Q \left(x \gamma^{aej} \gamma^{ah} \sum_{j=1}^{t} b_j \beta_j^h \right)$$

$$= \frac{(q-1)N}{e\delta q^r} \sum_{\underline{b} \in H_r^*} \sum_{h=1}^{e} \sum_{y \in C_0^{(N,Q)}} \psi_Q \left(y \gamma^{ah} \sum_{j=1}^{t} b_j \beta_j^h \right).$$

Setting $g = \gamma^a$, we have

$$(q-1)N(H_r) = \frac{(q-1)n}{q^r} + \frac{(q-1)N}{e\delta q^r} \sum_{\underline{b} \in H_r^*} \sum_{h=1}^{e} \sum_{y \in C_0^{(N,Q)}} \psi_Q \left(yg^h \sum_{j=1}^{t} b_j \beta_j^h \right).$$

That is,

$$N(H_r) = \frac{N}{e\delta q^r} \sum_{\underline{b} \in H_r} \sum_{h=1}^{e} \eta_{g^h \sum_{j=1}^{t} b_j \beta_j^h}^{(N,Q)}. \tag{2}$$

Therefore, to compute the GHWs for the cyclic code $\mathcal{C}$, it suffices to determine the maximal value of the above sum of the Gauss periods for all $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$. The problem is difficult in general. However, when the Gauss periods in the sum take only a few values, it is hopeful to determine the GHWs completely. Thus, the value N is one of the key points in the computation and we will consider below the simplest cases where $N \in \{1, 2\}$. We first deal with the case that $e = t$.

V. PROOF OF (I) OF THEOREM 1

Recall that $\beta_j = \gamma^{\frac{Q-1}{t}\Delta_j}$ for $1 \le j \le t$ and $g = \gamma^a$. Define $\beta = \gamma^{\frac{Q-1}{t}}$. Since $\beta_j^t = 1$ for each $1 \le j \le t$ and β_j's are distinct, we can assume without loss of generality that $\beta_j = \beta^j$, $1 \le j \le t$. We may make a change of variables $\underline{b} = (b_1, \ldots, b_t) \mapsto \underline{y} = (y_1, \ldots, y_t)$ by $y_i = g^i \sum_{j=1}^{t} b_j \beta^{ij}, 1 \le i \le t$. It is easy to see that this defines an $\mathbb{F}_q$-isomorphism $\phi : \mathbb{F}_Q^t \longrightarrow \mathbb{F}_Q^t$. Thus Equation (2) can be written as

$$N(H_r) = \frac{N}{t\delta q^r} \sum_{\underline{y} \in \phi(H_r)} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}.$$

Define

$$\widetilde{N}(H_r) = \frac{N}{t\delta q^r} \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}.$$

Clearly,

$$\max\left\{ N(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\} = \max\left\{ \widetilde{N}(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}.$$

Hence, we can focus on the determination of

$$\begin{aligned} N_r &= \max\left\{ \widetilde{N}(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\} \\ &= \frac{N}{t\delta q^r} \max\left\{ F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}, \end{aligned} \tag{3}$$

where

$$F(H_r) = \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}. \tag{4}$$

Now we are ready to prove (i) of Theorem 1.

A. Proof of (i) of Theorem 1: $N = 1$

Proof: Since $N = 1$, by (1), we have $e\delta \mid (q-1)$ and hence $e = t \le q - 1$. Recall that

$$\eta_a^{(1,Q)} = \begin{cases} Q - 1 & \text{if } a = 0, \\ -1 & \text{if } a \ne 0. \end{cases}$$

For any $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ and any $1 \le h \le t$, define

$$V_h = \underbrace{\mathbb{F}_Q \times \cdots \times \mathbb{F}_Q}_{h-1} \times \underset{h}{\{0\}} \times \underset{h+1}{\mathbb{F}_Q} \times \ldots \times \underset{t}{\mathbb{F}_Q}$$

and

$$v_h := v_h(H_r) = \dim_{\mathbb{F}_q}(H_r \cap V_h).$$

Then, by Equation (4),

$$F(H_r) = \sum_{h=1}^{t} (|H_r \cap V_h|(Q-1) - (q^r - |H_r \cap V_h|))$$

$$= \sum_{h=1}^{t} q^{v_h}((Q-1) - (q^r - q^{v_h}))$$

$$= Q \sum_{h=1}^{t} q^{v_h} - tq^r.$$

Hence, for any r-dimensional subspace H_r, the tuple $(v_1(H_r), \ldots, v_t(H_r))$ completely determines $F(H_r)$.

To find $\max \left\{ F(H_r) : H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}$, we may assume that $v_1 \geq v_2 \geq \cdots \geq v_t$, since the ordering of v_h's does not affect the value. We perform the following procedure successively: first we find H_r's that maximize the value $v_1 = v_1(H_r)$; once $v_1, \ldots, v_i$ are determined for $i \geq 1$, then among the H_r's we find the ones that maximize v_{i+1}. Since $t \leq q-1$, it is easy to see that this procedure will produce the desired H_r which maximizes $F(H_r)$.

Now suppose $(t-s-1)m < r \leq (t-s)m$ for some s in the range $0 \leq s \leq t-1$. Noting that

$$\dim_{\mathbb{F}_q} \left(\bigcap_{i=1}^{s} V_i \right) = (t-s)m, \quad \dim_{\mathbb{F}_q} \left(\bigcap_{i=1}^{s+1} V_i \right) = (t-s-1)m,$$

we may take $v_1 = \ldots = v_s = r$, which are obviously maximal. This means that $H_r \subset \bigcap_{i=1}^{s} V_i$. To make v_{s+1} maximal, we shall take $\bigcap_{i=1}^{s+1} V_i \subset H_r \subset \bigcap_{i=1}^{s} V_i$, so that $v_{s+1} = (t-s-1)m$. Under this configuration, H_r is of the form

$$H_r = \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{H} \times \underset{s+2}{\mathbb{F}_Q} \times \ldots \times \underset{t}{\mathbb{F}_Q},$$

where $H \subset \mathbb{F}_Q$ is any $\mathbb{F}_q$-vector space of dimension $r - (t-s-1)m$, and we find

$$v_h = v_h(H_r) = \begin{cases} r & 1 \leq h \leq s, \\ (t-s-1)m & h = s+1, \\ r-m & s+2 \leq h \leq t. \end{cases}$$

Therefore we obtain

$$\max \left\{ F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\} = Q \left(sq^r + q^{(t-s-1)m} + (t-s-1)q^{r-m} \right) - tq^r,$$

and

$$d_r = n - \frac{1}{t\delta q^r} \max \left\{ F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}$$

$$= \frac{q^m - 1}{\delta}\left(1 - \frac{s}{t}\right) - \frac{q^{(t-s)m-r} - 1}{t\delta}.$$

This completes the proof of (i) of Theorem 1. ∎

VI. PROOF OF (II) OF THEOREM 1: $N = 2$

For $t = e \geq 1$ and $N = 2$, the situation is more difficult. We first adopt a new strategy that works for any $N \geq 2$. This strategy was inspired by [57].

A. A new strategy

Let $\langle \cdot, \cdot \rangle : \mathbb{F}_Q^t \times \mathbb{F}_Q^t \to \mathbb{F}_q$ be the non-degenerate bilinear form given by

$$\langle \underline{x}, \underline{y} \rangle = \mathrm{Tr}_q^Q \left(\sum_{i=1}^{t} x_i y_i \right), \quad \forall \underline{x} = (x_1, \ldots, x_t), \underline{y} = (y_1, \ldots, y_t) \in \mathbb{F}_Q^t.$$

Then for any $\mathbb{F}_q$-subspace H of $\mathbb{F}_Q^t$, we define

$$H^\perp = \{ y \in \mathbb{F}_Q^t \mid \langle \underline{x}, \underline{y} \rangle = 0, \forall \underline{x} \in H \}.$$

We have the following lemma.

Lemma 4. *Suppose $H \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$. Then $\dim_{\mathbb{F}_q} H^{\perp} = tm - r$ and*

$$\frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^{\perp}} \psi_q\left(\langle \underline{x}, \underline{y} \rangle\right) = \begin{cases} 1 & \text{if } \underline{x} \in H, \\ 0 & \text{if } \underline{x} \notin H. \end{cases}$$

Proof: Let $A = \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^{\perp}} \psi_q(\langle \underline{x}, \underline{y} \rangle)$. If $\underline{x} \in H$, then $\langle \underline{x}, \underline{y} \rangle = 0$, $\forall \underline{y} \in H^{\perp}$. Hence, $A = 1$. If $\underline{x} \notin H$, then there exists $\underline{y} \in H^{\perp}$ such that $\langle \underline{x}, \underline{y} \rangle \neq 0$. In particular, there exists $\underline{y_0} \in H^{\perp}$, such that $\psi_q(\langle \underline{x}, \underline{y_0} \rangle) \neq 1$. Thus,

$$A \cdot \psi_q(\langle \underline{x}, \underline{y_0} \rangle) = \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^{\perp}} \psi_q(\langle \underline{x}, \underline{y} \rangle + \langle \underline{x}, \underline{y_0} \rangle)$$

$$= \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^{\perp}} \psi_q(\langle \underline{x}, \underline{y} + \underline{y_0} \rangle) = A.$$

Hence $A = 0$. This completes the proof. ∎

By the above lemma, we can compute $F(H_r)$ in Equation (4) as follows.

$$F(H_r) = \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)} = \sum_{h=1}^{t} \sum_{\underline{y} \in \mathbb{F}_Q^t} \eta_{y_h}^{(N,Q)} \frac{1}{q^{tm-r}} \sum_{\underline{x} \in H_r^{\perp}} \psi_q(\langle \underline{x}, \underline{y} \rangle)$$

$$= \frac{1}{q^{tm-r}} \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^{\perp}} \sum_{z \in C_0^{(N,Q)}} \sum_{\underline{y} \in \mathbb{F}_Q^t} \psi_Q(zy_h) \psi_q\left(\text{Tr}_q^Q\left(\sum_{i=1}^{t} x_i y_i\right)\right)$$

$$= \frac{1}{q^{tm-r}} \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^{\perp}} \sum_{z \in C_0^{(N,Q)}} \sum_{y_1,\ldots,y_t \in \mathbb{F}_Q} \psi_Q\left(zy_h + \sum_{i=1}^{t} x_i y_i\right)$$

$$= q^r \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^{\perp}} \sum_{\substack{z \in C_0^{(N,Q)} \\ z + x_h = 0 \\ x_i = 0, \forall i \neq h}} 1.$$

For any $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ and $1 \leq h \leq t$, define

$$W_h := W_h(N) = \underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underbrace{(-C_0^{(N,Q)})}_{h} \times \underbrace{\{0\}}_{h+1} \times \cdots \underbrace{\{0\}}_{t}$$

and

$$U_h := U_h(H_r) = H_r^{\perp} \bigcap \left(\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underbrace{\mathbb{F}_Q}_{h} \times \underbrace{\{0\}}_{h+1} \times \cdots \underbrace{\{0\}}_{t} \right).$$

Then we have

$$F(H_r) = q^r \sum_{h=1}^{t} |H_r^{\perp} \cap W_h| = q^r \sum_{h=1}^{t} |U_h \cap W_h|. \tag{5}$$

Therefore for $t = e \geq 1$ and $N \geq 2$, to compute the GHWs, it suffices to determine the maximal value of $\sum_{h=1}^{t} |U_h \cap W_h|$ for all $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$.

We remark that since $H_r^{\perp} = \bigoplus_{h=1}^{t} U_h$, the spaces $H_r^{\perp}$ and H_r can be uniquely recovered from $(U_1, \ldots, U_t)$, where U_h is a subspace of $\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underbrace{\mathbb{F}_Q}_{h} \times \underbrace{\{0\}}_{h+1} \times \cdots \{0\}_t$. Setting $r' = tm - r$ and letting $u_h = \dim_{\mathbb{F}_q}(U_h)$, the u_h's satisfy the condition that $\sum_{h=1}^{t} u_h = r'$. So to find the maximal value of $\sum_{h=1}^{t} |U_h \cap W_h|$, we consider the following two steps:

1). for each eligible tuple $(u_1, \ldots, u_h)$, determine the spaces U_h of dimension u_h such that $|U_h \cap W_h|$ is maximal for each h;

2). consider all eligible tuples $(u_1, \ldots, u_h)$ and find the maximal.

Now we focus on the case that $N = 2$.

B. A working lemma

Since $N = 2$, q is odd and m is even. Note that $Q = q^m$. We need the following lemma.

Lemma 5. *Let $0 \le l \le m$ and $H \subset \mathbb{F}_Q$ be an l-dimensional $\mathbb{F}_q$-subspace. Let γ be a primitive element of $\mathbb{F}_Q$. Define a function*

$$f(l) := \begin{cases} q^l - 1 & \text{if } 0 \le l \le \frac{m}{2}, \\ \frac{q^l - 1}{2} + \frac{q^{\frac{m}{2}} - q^{l - \frac{m}{2}}}{2} & \text{if } \frac{m}{2} \le l \le m. \end{cases}$$

Then, for $0 \le l \le m$,

$$\max \left\{ \left| H \cap C_i^{(2,Q)} \right| : H \subset \mathbb{F}_Q, \dim_{\mathbb{F}_q}(H) = l \right\} = f(l),$$

where $i \in \{0, 1\}$. Furthermore, the subspace $H \subset \mathbb{F}_Q$ that achieves the maximal value can be chosen as follows:

1) *If $0 \le l \le \frac{m}{2}$, then we can choose any $H \subset \gamma^i \mathbb{F}_{q^{\frac{m}{2}}}$;*

2) *If $\frac{m}{2} \le l \le m$, suppose $G(\chi) = (-1)^j q^{\frac{m}{2}}$ for some $j \in \{0, 1\}$, where χ is the quadratic character of $\mathbb{F}_Q$. Then we can choose H satisfying $H^\perp \subset C_{i+j}^{(2,Q)} \cup \{0\}$, here $H^\perp$ is the orthogonal complement of H with respect to the non-degenerate bilinear form $\langle \cdot, \cdot \rangle : \mathbb{F}_Q \times \mathbb{F}_Q \to \mathbb{F}_q$ given by*

$$\langle x, y \rangle = Tr_q^Q(xy), \forall x, y \in \mathbb{F}_Q.$$

Proof: We will only prove the lemma for the case $i = 0$. The case of $i = 1$ is analogous.

If $0 \le l \le \frac{m}{2}$, then $\mathbb{F}_{q^{\frac{m}{2}}}^* \subset C_0^{(2,Q)}$. Note that $\dim_{\mathbb{F}_q}\left(\mathbb{F}_{q^{\frac{m}{2}}}\right) = \frac{m}{2}$. For any $H \subset \mathbb{F}_{q^{\frac{m}{2}}}$, we have $|H \cap C_0^{(2,Q)}| = q^l - 1$, which is clearly the maximal value.

If $\frac{m}{2} \le l \le m$, then

$$|H \cap C_0^{(2,Q)}| = \sum_{a \in H \setminus \{0\}} \frac{1}{2}(1 + \chi(a)) = \frac{q^l - 1}{2} + \frac{1}{2} \sum_{a \in H} \chi(a).$$

Note that

$$\sum_{a \in H} \chi(a) = \sum_{a \in \mathbb{F}_Q} \frac{\chi(a)}{q^{m-l}} \sum_{b \in H^\perp} \psi_q(\langle a, b \rangle)$$

$$= \frac{1}{q^{m-l}} \sum_{b \in H^\perp} \chi(b) \sum_{a \in \mathbb{F}_Q} \chi(ab) \psi_q(\langle a, b \rangle)$$

$$= \frac{G(\chi)}{q^{m-l}} \sum_{b \in H^\perp} \chi(b).$$

Since $\dim_{\mathbb{F}_q}(H^\perp) = m - l \le \frac{m}{2}$, we can choose $H^\perp$ satisfying $H^\perp \subset C_j^{(2,Q)} \cup \{0\}$. Consequently, we have $\chi(b) = (-1)^j$, $\forall b \in H^\perp \setminus \{0\}$. Hence,

$$\sum_{a \in H} \chi(a) = \frac{q^{\frac{m}{2}}}{q^{m-l}} \sum_{b \in H^\perp \setminus \{0\}} 1 = q^{\frac{m}{2}} - q^{l - \frac{m}{2}}.$$

This is clearly the largest value of $\sum_{a \in H} \chi(a)$. Therefore,

$$\left| H \cap C_0^{(2,Q)} \right| = \frac{q^l - 1}{2} + \frac{q^{\frac{m}{2}} - q^{l - \frac{m}{2}}}{2} = f(l)$$

is the maximal value when $\frac{m}{2} \le l \le m$. This finishes the proof of Lemma 5. ∎

C. Proof of (ii) of Theorem 1

We can now start the proof of (ii) of Theorem 1. Recall that H_r can be recovered from $(U_1, \ldots, U_t)$ where U_h's are subspaces of dimension u_h such that $\sum_{h=1}^t u_h = r' = tm - r$. For any eligible fixed tuple $(u_1, \ldots, u_t)$, Lemma 5 tells us how to choose $(U_1, \ldots, U_t)$ so that $|U_h \cap W_h|$ attains the maximal value $f(u_h)$ for each $1 \le h \le t$. Hence it remains to determine which tuple $(u_1, \ldots, u_t)$ will give the maximal value $\sum_{h=1}^t f(u_h)$, here $(u_1, \ldots, u_t)$ satisfies the condition that $0 \le u_h \le m, \forall h$ and $\sum_{h=1}^t u_h = r'$. We may assume without loss of generality that $u_1 \ge \cdots \ge u_t$.

The following lemma is useful to determine the maximal value of $\sum_{h=1}^t f(u_h)$. We define a finite set $\mathcal{L} = \{(l_1, \ldots, l_t) \mid 0 \le l_1, \ldots, l_t \le m, l_1 \ge l_2 \ge \cdots \ge l_t\}$ and for each $0 \le s \le tm$ a subset $\mathcal{L}_s = \{(l_1, \ldots, l_t) \in \mathcal{L} \mid \sum_{i=1}^t l_i = s\}$. We can define a partial order on $\mathcal{L}_s$ as follows: for any $\underline{l} = (l_1, \ldots, l_t), \underline{l}' = (l'_1, \ldots, l'_t) \in \mathcal{L}_s$, we say $\underline{l} \succ \underline{l}'$ if there is an index i $(1 \le i \le t)$, such that $l_j = l'_j, \forall 1 \le j \le i - 1$ and $l_i > l'_i$. It is easy to see that $\succ$ gives a total order on $\mathcal{L}_s$.

Lemma 6. *For any $\underline{l}, \underline{l}' \in \mathcal{L}_s$, if $\underline{l} \succ \underline{l}'$, then $\sum_{h=1}^t f(l_h) \geq \sum_{h=1}^t f(l'_h)$.*

Proof: For any $\underline{l} = (l_1, \ldots, l_t) \in \mathcal{L}_s$, define $f(\underline{l}) = \sum_{h=1}^t f(l_h)$. For simplicity define $l_0 := m$. Suppose $l_i < l_{i-1}$ and $l_j \geq 1$ for some i, j such that $1 \leq i < j \leq t$. Then we can define an operation $S_{i,j}$ on $\underline{l}$ as follows:

$$S_{i,j}(\underline{l}) = (l_1, \ldots, l_{i-1}, l_i + 1, l_{i+1}, \ldots, l_{j-1}, l_j - 1, l_{j+1}, \ldots, l_t).$$

Clearly $S_{i,j}(\underline{l}) \in \mathcal{L}_s$ and $S_{i,j}(\underline{l}) \succ \underline{l}$. We claim that $f(S_{i,j}(\underline{l})) \geq f(\underline{l})$.

It suffices to prove that

$$f(l_i + 1) - f(l_i) \geq f(l_j) - f(l_j - 1), \quad l_i \geq l_j \geq 1. \tag{6}$$

For $1 \leq l \leq m$, define a function $g(l) = f(l) - f(l-1)$. A routine computation shows easily that g is an increasing function. Therefore, the above inequality (6) holds. Hence the claim is proved.

Finally, Lemma 6 is proved by realizing that for any $\underline{l} \succ \underline{l}'$, $\underline{l}$ can be obtained from $\underline{l}'$ by a series of operations $S_{i,j}$ for some i, j's. ∎

Armed with Lemma 6, we can prove (ii) of Theorem 1 as follows: suppose $(t - s - 1)m < r \leq (t - s)m$ for some $0 \leq s \leq t - 1$, then $sm \leq r' = tm - r < (s+1)m$. We can choose an $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, such that

$$H_r^\perp = \underbrace{\mathbb{F}_Q \times \cdots \times \mathbb{F}_Q}_{s} \times \underset{s+1}{T} \times \underset{s+2}{\{0\}} \times \cdots \times \underset{t}{\{0\}},$$

where T is an $(r' - sm)$-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_Q$. For $1 \leq h \leq t$,

$$U_h = H_r^\perp \cap (\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{\mathbb{F}_Q} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}})$$

is of the form

$$U_h = \underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{Y_h} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}},$$

where Y_h is an $\mathbb{F}_q$-subspace of $\mathbb{F}_Q$. We can further require that for each $1 \leq h \leq t$, $\left| Y_h \cap (-C_0^{(2,Q)}) \right|$ achieves the maximal value as discussed in Lemma 5. Therefore, by Equation (5), $F(H_r) = \sum_{h=1}^t f(u_h)$, where $u_1 = \cdots = u_s = m$, $u_{s+1} = r' - sm = (t-s)m - r$ and $u_{s+2} = \cdots = u_t = 0$. Clearly $\underline{u} = (u_1, \ldots, u_t) \in \mathcal{L}_{r'}$ is the maximum according to the order $\succ$. Then by Lemma 6, the value $F(H_r)$ is maximal, namely, this H_r is the r-dimensional subspace that maximizes $F(H_r)$ for all $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$. By Equation (3) and Lemma 5, we obtain

$$N_r = \frac{2}{t\delta} \left[\frac{s(q^m - 1)}{2} + f((t-s)m - r) \right].$$

This completes the proof of (ii) of Theorem 1.

VII. PROOF OF THEOREM 2

In this section, we consider the case $e > t$ and $N = 1$. If $t = 1$, the code $\mathcal{C}$ is irreducible which was considered in [57]. So we may assume that $e > t \geq 2$. Recall that for $1 \leq r \leq tm$ and $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, by Equation (2) we have

$$N(H_r) = \frac{1}{e\delta q^r} \sum_{\underline{b} \in H_r} \sum_{h=1}^e \eta_{g^h \sum_{j=1}^t b_j \beta_j^h}^{(1,Q)},$$

where $g = \gamma^a$, $\beta = \gamma^{\frac{Q-1}{e}}$ and $\beta_j = \beta^{\Delta_j}$ for $1 \leq j \leq t$. For $1 \leq h \leq e$, define

$$W_h := \left\{ \underline{b} = (b_1, \ldots, b_t) \in \mathbb{F}_Q^t : \sum_{j=1}^t b_j \beta_j^h = 0 \right\}.$$

Then each W_h is an $\mathbb{F}_q$-vector space of dimension $(t-1)m$. Let

$$w_h := \dim_{\mathbb{F}_q}(H_r \cap W_h).$$

Since $\eta_0^{(1,Q)} = Q - 1$ and $\eta_y^{(1,Q)} = -1$ if $y \in \mathbb{F}_Q^*$, we have

$$N(H_r) = \frac{1}{e\delta q^r} \sum_{h=1}^{e} \left((Q-1)q^{w_h} - (q^r - q^{w_h}) \right)$$

$$= \frac{1}{e\delta q^r} \left(Q \sum_{h=1}^{e} q^{w_h} - eq^r \right) = \frac{Q}{e\delta q^r} \sum_{h=1}^{e} q^{w_h} - \frac{1}{\delta}. \tag{7}$$

To find $\max \left\{ N(H_r) : H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}$, we may assume without loss of generality that $w_1 \geq w_2 \geq \ldots \geq w_e$. We make a change of variables $\underline{b} = (b_1, \ldots, b_t) \mapsto \underline{y} = (y_1, \ldots, y_t)$ given by $y_h = g^h \sum_{j=1}^{t} b_j \beta_j^h, 1 \leq h \leq t$. This clearly defines an $\mathbb{F}_q$-isomorphism $\phi : \mathbb{F}_Q^t \to \mathbb{F}_Q^t$. For $t + 1 \leq h \leq e$, define $y_h := g^h \sum_{j=1}^{t} b_j \beta_j^h$. Since ϕ is an isomorphism, there exist $\lambda_{h,1}, \ldots, \lambda_{h,t} \in \mathbb{F}_Q$ such that

$$y_h = \sum_{i=1}^{t} \lambda_{h,i} y_i, \quad t + 1 \leq h \leq e.$$

Since $\{\Delta_1 \pmod{e}, \ldots, \Delta_t \pmod{e}\}$ is an arithmetic progression, it is known that $\lambda_{h,i} \neq 0, \forall h, i$ where $t + 1 \leq h \leq e, 1 \leq i \leq t$ (see [55]).

Thus Equation (7) can be written as

$$N(H_r) = \frac{Q}{e\delta q^r} \sum_{h=1}^{e} q^{\widetilde{w}_h} - \frac{1}{\delta},$$

where

$$\widetilde{w}_h := \dim_{\mathbb{F}_q} \left(\widetilde{H}_r \cap \widetilde{W}_h \right) \text{ and } \widetilde{w}_1 \geq \widetilde{w}_2 \geq \ldots \geq \widetilde{w}_e.$$

Here $\widetilde{H}_r = \phi(H_r)$ and $\widetilde{W}_h = \phi(W_h)$ is of the form

$$\widetilde{W}_h = \underbrace{\mathbb{F}_Q \times \cdots \mathbb{F}_Q}_{h-1} \times \underset{h}{\{0\}} \times \underset{h+1}{\mathbb{F}_Q} \times \cdots \times \underset{t}{\mathbb{F}_Q}, \quad 1 \leq h \leq t,$$

and

$$\widetilde{W}_h = \left\{ (y_1, \cdots, y_t) \in \mathbb{F}_Q^t : y_h = \sum_{i=1}^{t} \lambda_{h,i} y_i = 0 \right\}, \quad t + 1 \leq h \leq e.$$

Since $e \leq q - 1$, to find the H_r that maximizes $N(H_r)$, similar to the case that $e = t$ and $N = 1$, the first priority is to make $\widetilde{w}_1$ as large as possible, once this is done, then we make $\widetilde{w}_2$ as large as possible, etc, and finally we make $\widetilde{w}_e$ as large as possible.

Now suppose that $(t - s - 1)m < r \leq (t - s)m$ for some $0 \leq s \leq t - 1$. Since $\dim_{\mathbb{F}_q} \left(\bigcap_{h=1}^{s} \widetilde{W}_h \right) = (t - s)m$, similar to the case that $e = t$ and $N = 1$, $N(H_r)$ achieves the maximal value for $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ satisfying the property that $\bigcap_{h=1}^{s+1} \widetilde{W}_h \subset \widetilde{H}_r \subset \bigcap_{h=1}^{s} \widetilde{W}_h$. Consequently, $\widetilde{H}_r$ is of the form

$$\widetilde{H}_r = \begin{cases} \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{T} \times \underset{s+2}{\mathbb{F}_Q} \times \cdots \times \underset{t}{\mathbb{F}_Q} & \text{if } 0 \leq s \leq t - 2, \\ \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{T} & \text{if } s = t - 1. \end{cases}$$

Here T is an $\mathbb{F}_q$-subspace of $\mathbb{F}_Q$ with dimension $r - (t - s - 1)m$.

If $0 \leq s \leq t - 2$, it is easy to check that $\widetilde{w}_1 = \cdots = \widetilde{w}_s = r$, $\widetilde{w}_{s+1} = (t - s - 1)m$ and $\widetilde{w}_{s+2} = \cdots = \widetilde{w}_t = r - m$. For $t + 1 \leq h \leq e$, $\widetilde{w}_h$, by definition, is the $\mathbb{F}_q$-dimension of the space of $(y_{s+1}, \ldots, y_t)$ such that

$$\lambda_{h,s+1} y_{s+1} + \lambda_{h,s+2} y_{s+2} + \cdots + \lambda_{h,t} y_t = 0,$$

where $y_{s+1} \in T$ and $y_{s+2}, \ldots, y_t \in \mathbb{F}_Q$. Since $\forall h, i, \lambda_{h,i} \neq 0$, it is easy to see $\widetilde{w}_h = r - m$ for $t + 1 \leq h \leq e$. Therefore this H_r maximizes $\sum_{h=1}^{e} q^{\widetilde{w}_h}$ whose value is given by

$$\sum_{h=1}^{e} q^{\widetilde{w}_h} = sq^r + q^{(t-s-1)m} + (e - s - 1)q^{r-m}.$$

If $s = t - 1$, we can see that $\widetilde{w}_1 = \cdots = \widetilde{w}_s = r$ and $\widetilde{w}_{s+1} = 0$. Hence for any $s + 2 \leq h \leq e$, by the inequality $0 \leq \widetilde{w}_h \leq \widetilde{w}_{s+1}$, we also have $\widetilde{w}_h = 0$ for $s + 2 \leq h \leq e$. That is, the H_r maximizes $\sum_{h=1}^{e} q^{\widetilde{w}_h}$ whose value is given by

$$\sum_{h=1}^{e} q^{\widetilde{w}_h} = sq^r + e - s.$$

Then a routine computation completes the proof.

VIII. Conclusion

The generalized Hamming weights (GHWs) are fundamental parameters of linear codes. They convey the structural information of a linear code and determine its performance in various applications. However, the computation of the GHWs of linear codes is difficult in general. In this paper, we study the GHWs of a family of reducible codes introduced in [55] and obtain the weight hierarchy in several cases. This is achieved by extending the idea of [57] into higher dimension and by employing some interesting combinatorial arguments. It shall be noted that these cyclic codes may have arbitrary number of nonzeroes.

References

[1] A. Ashikhmin, A. Barg, and S. Litsyn. New upper bounds on generalized weights. *IEEE Trans. Inform. Theory*, 45(4):1258–1263, 1999.

[2] A. I. Barbero and C. Munuera. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.*, 13(1):79–104, 2000.

[3] M. Bras-Amorós, K. Lee, and A. Vico-Oton. New lower bounds on the generalized Hamming weights of AG codes. *IEEE Trans. Inform. Theory*, 60(10):5930–5937, 2014.

[4] J. Cheng and C. Chao. On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two. *IEEE Trans. Inform. Theory*, 43(1):294–299, 1997.

[5] J. P. Cherdieu, D. J. Mercier, and T. Narayaninsamy. On the generalized weights of a class of trace codes. *Finite Fields Appl.*, 7(2):355–371, 2001.

[6] H. Chung. The 2-nd generalized Hamming weight of double-error correcting binary BCH codes and their dual codes. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 118–129. Springer, Berlin, 1991.

[7] G. Cohen, S. Litsyn, and G. Zémor. Upper bounds on generalized distances. *IEEE Trans. Inform. Theory*, 40(6):2090–2092, 1994.

[8] M. Delgado, J. I. Farrán, P. A. García-Sánchez, and D. Llena. On the weight hierarchy of codes coming from semigroups with two generators. *IEEE Trans. Inform. Theory*, 60(1):282–295, 2014.

[9] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 21(5):575–576, 1975.

[10] I. Duursma, H. Stichtenoth, and C. Voß. Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 53–65. de Gruyter, Berlin, 1996.

[11] G. L. Feng, K. K. Tzeng, and V. K. Wei. On the generalized Hamming weights of several classes of cyclic codes. *IEEE Trans. Inform. Theory*, 38(3):1125–1130, 1992.

[12] G. D. Forney. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, 40(6):1741–1752, 1994.

[13] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. *SIAM J. Comput.*, 40(5):1432–1462, 2011.

[14] C. Güneri and F. Özbudak. Improvements on generalized Hamming weights of some trace codes. *Des. Codes Cryptogr.*, 39(2):215–231, 2006.

[15] V. Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[16] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[17] T. Helleseth and T. Kløve. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 42(3):1029–1034, 1996.

[18] T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus. Bounds on the minimum support weights. *IEEE Trans. Inform. Theory*, 41(2):432–440, 1995.

[19] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block length $n_1((q^l - 1)/N)$. *Discrete Math.*, 18(2):179–211, 1977.

[20] T. Helleseth, T. Kløve, and Ø. Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inform. Theory*, 38(3):1133–1140, 1992.

[21] T. Helleseth and P. Vijay Kumar. The weight hierarchy of the Kasami codes. *Discrete Math.*, 145(1-3):133–143, 1995.

[22] T. Helleseth and P. Vijay Kumar. On the weight hierarchy of the semiprimitive codes. *Discrete Math.*, 152(1-3):185–190, 1996.

[23] J. W. P. Hirschfeld, M. A. Tsfasman, and S. G. Vladut. The weight hierarchy of higher dimensional hermitian codes. *IEEE Trans. Inform. Theory*, 40(1):275–278, 1994.

[24] M. Homma and S. J. Kim. The second generalized Hamming weight for two-point codes on a Hermitian curve. *Des. Codes Cryptogr.*, 50(1):1–40, 2009.

[25] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[26] H. Janwa and A. K. Lal. On the generalized Hamming weights of cyclic codes. *IEEE Trans. Inform. Theory*, 43(1):299–308, 1997.

[27] H. Janwa and A. K. Lal. On generalized Hamming weights and the covering radius of linear codes. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, pages 347–356. Springer, Berlin, 2007.

[28] T. Kasami, T. Takata, T. Fujiwara, and S. Lin. On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes. *IEEE Trans. Inform. Theory*, 39(1):242–245, 1993.

[29] T. Kløve. The weight distribution of linear codes over $\mathrm{GF}(q^l)$ having generator matrix over $\mathrm{GF}(q)$. *Discrete Math.*, 23(2):159–168, 1978.

[30] J. Kurihara and T. Uyematsu. Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight. In *49th Annual Allerton Conference on Communication, Control, and Computing*, pages 951–957, Sep 2011.

[31] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[32] C. Martínez-Pérez and W. Willems. On the weight hierarchy of product codes. *Des. Codes Cryptogr.*, 33(2):95–108, 2004.

[33] O. Moreno, J. P. Pedersen, and D. Polemi. An improved Serre bound for elementary abelian extensions of $F_q(x)$ and the generalized Hamming weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, 44(3):1291–1293, 1998.

[34] C. Munuera. On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(6):2092–2099, 1994.

[35] C. Munuera and D. Ramirez. The second and third generalized Hamming weights of Hermitian codes. *IEEE Trans. Inform. Theory*, 45(2):709–712, 1999.

[36] C. Ngai, R. W. Yeung, and Z. Zhang. Network generalized Hamming weight. *IEEE Trans. Inform. Theory*, 57(2):1136–1143, 2011.

[37] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. In *Advances in cryptology (Paris, 1984)*, volume 209 of *Lecture Notes in Comput. Sci.*, pages 33–50. Springer, Berlin, 1985.

[38] J. Y. Park. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 46(6):2228–2235, 2000.

[39] S. El Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory*, 58(3):1361–1371, 2012.

[40] H. G. Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 46(7):2648–2651, 2000.

[41] H. G. Schaathun and W. Willems. A lower bound on the weight hierarchies of product codes. *Discrete Appl. Math.*, 128(1):251–261, 2003.

[42] C. Shim and H. Chung. On the second generalized Hamming weight of the dual code of a double-error-correcting binary BCH code. *IEEE Trans. Inform. Theory*, 41(3):805–808, 1995.

[43] H. Stichtenoth and C. Voß. Generalized Hamming weights of trace codes. *IEEE Trans. Inform. Theory*, 40(2):554–558, 1994.

[44] M. A. Tsfasman and S. G. Vlăduţ. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6):1564–1588, 1995.

[45] G. van der Geer and M. van der Vlugt. Generalized Hamming weights of Melas codes and dual Melas codes. *SIAM J. Discrete Math.*, 7(4):554–559, 1994.

[46] G. van der Geer and M. van der Vlugt. On generalized Hamming weights of BCH codes. *IEEE Trans. Inform. Theory*, 40(2):543–546, 1994.

[47] G. van der Geer and M. van der Vlugt. Fibre products of Artin-Schreier curves and generalized Hamming weights of codes. *J. Combin. Theory Ser. A*, 70(2):337–348, 1995.

[48] G. van der Geer and M. van der Vlugt. Generalized hamming weights of BCH(3) revisited. *IEEE Trans. Inform. Theory*, 41(1):300–301, 1995.

[49] G. van der Geer and M. van der Vlugt. The second generalized Hamming weight of the dual codes of double-error correcting binary BCH-codes. *Bull. London Math. Soc.*, 27(1):82–86, 1995.

[50] G. van der Geer and M. van der Vlugt. Quadratic forms, generalized Hamming weights of codes and curves with many points. *J. Number Theory*, 59(1):20–36, 1996.

[51] M. van der Vlugt. On the weight hierarchy of irreducible cyclic codes. *J. Combin. Theory Ser. A*, 71(1):159–167, 1995.

[52] M. van der Vlugt. A note on generalized Hamming weights of BCH(2). *IEEE Trans. Inform. Theory*, 42(1):254–256, 1996.

[53] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

[54] V. K. Wei and K. Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993.

[55] J. Yang, M. Xiong, C. Ding, and J. Luo. Weight distribution of a class of cyclic codes with arbitrary number of zeros. *IEEE Trans. Inform. Theory*, 59(9):5985–5993, 2013.

[56] K. Yang, P. Vijay Kumar, and H. Stichtenoth. On the weight hierarchy of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(3):913–920, 1994.

[57] M. Yang, J. Li, K. Feng, and D. Lin. Generalized Hamming weights of irreducible cyclic codes. arXiv:1410.2702.